안전한 사물인터넷 구축

안전과 신뢰성 보장, 혁신 추구

Steve Hanna
Senior Principal Technical Marketing

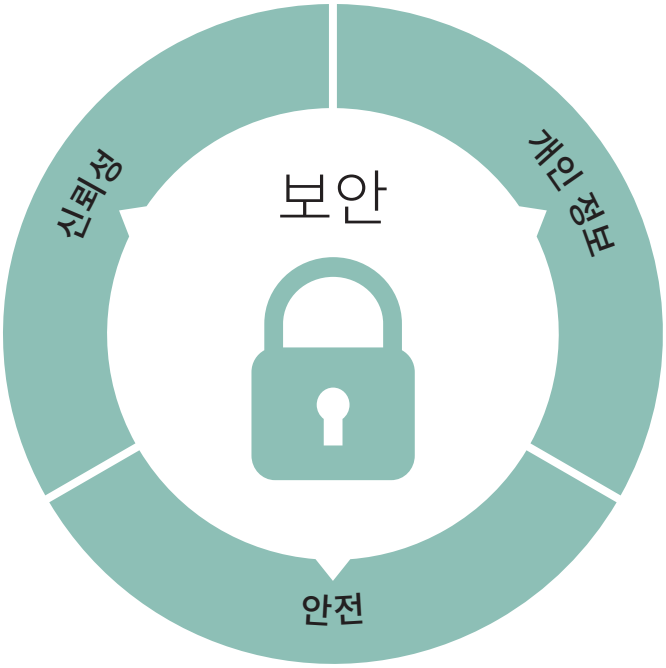
www.infineon.com/IoT-Security

개요

새롭게 떠오르는 사물 인터넷(IoT)은 혁신적인 기업들이 더 효율적인 산업과 안전한 교통을 구현하면서 사람들의 일상생활을 보다 편리하고 만족스럽게 만들어주는 제품과 서비스를 제공할 수 있는 막대한 기회를 열어줍니다. 하지만 이점이 큰 만큼 위험도 큽니다. 공장, 가정, 자동차 그리고 도시에서 원격으로 수행되는 지능적인 모니터링과 제어는 효율과 편리함을 증대시킬 수 있지만, 똑같이 강력한 도구가 악의적인 집단에 의해 중요한 인프라를 파괴하는 데 악용됨으로써 높은 위험과 비용이 초래될 수 있습니다. 개인적인 차원에서 IoT는 가정과 개인의 정보를 악의적이거나 범죄적인 행위에 노출시킬 수 있습니다.

다행히 다른 분야에서 지난 수십 년에 걸쳐 개발된 보안 기법들을 IoT에 적용할 수 있습니다. 이러한 기법은 지속적인 혁신을 추구하면서 효과적이고 비용 효율적인 보호를 제공하는 검증된 성과를 보여주고 있습니다.

IoT 분야에 종사하는 많은 개발자들은 보안 전문가가 아니며 생산, 자동차, 가전기기 또는 다른 분야의 전문가들입니다. 개발자들은 제품에 보안을 포함시켜야 하지만, 보안 역시 해당되는 분야의 요구사항을 만족시켜야 합니다. 이와 같은 점이 인피니언과 같은 보안 솔루션 전문업체가 사물 인터넷과 관련된 다양한 분야에 참여하여 처음부터 강력하고 적합한 보안을 구축하도록 보장하는 이유입니다. 보안을 구축하면 우리 모두가 중요하게 생각하는 안전, 신뢰성, 개인 정보의 가치를 보호할 수 있습니다.



차례

1. 동기

사물 인터넷(IoT)은 21세기에 가장 중요한 기술 동향으로 꼽을 수 있습니다. IoT는 수십억 개의 전자 센서와 제어 요소들을 상호간, 그리고 상호 연결된 네트워크에 연결함으로써 전 세계의 모든 시민들을 위해 효율과 편리함을 증대시키고 라이프스타일을 향상시키는 데 기여하게 될 것입니다. 사물 인터넷의 영향은 공장의 생산 현장에서부터 사무실 건물, 소매점, 대중 교통 시스템과 커넥티드 카, 그리고 우리들의 가정에서도 볼 수 있습니다.

IoT 역시 과거의 기술 향상과 마찬가지로 위험한 측면을 동시에 갖고 있습니다. 가까운 미래에 다음과 같은 가능한 시나리오를 상상할 수 있습니다.

마리아 솔라노(Maria Solano)*는 유쾌하지 않은 하루를 보냈다. 평소와 다르게 심하게 막히는 교통으로 직장에 15분 늦었다. 아침의 짧은 휴식 시간에 뉴스에서 그 지역 교통 조정 시스템에 컴퓨터 고장이 발생해 교통 신호 동기화가 작동하지 않았다는 보도를 들었다. 점심 시간에는 집에 있는 쌍둥이들을 보기 위해 인터넷에 연결된 홈 비디오 모니터에 들어가려 했지만 로그인이 되지 않아 당황했다. 유모에게 전화를 걸자 집안 모니터에서 이상한 목소리가 들려 최선책으로 모니터 전원을 껐다는 설명을 들었다. 그녀는 재빨리 가족의 비공식적인 IT 전문가인 남편에게 전화를 걸어 무엇이 잘못된 건지 물어보았다.

공장에서는 더 심각한 일이 발생했다. 공장 생산 현장의 자동화된 페인트 라인에서 페인트 스프레이어가 제멋대로 시작과 정지를 반복하는 일이 일어나 결국 라인을 정지시켰고 고가의 손실이 발생했다. 마리아는 오후 내내 생산 관리자와 IT 수퍼바이저와 함께 문제의 원인을 찾는 데 보냈으며 멀웨어가 침투한 것을 밝혀냈다. 아무도 확신할 수는 없었지만, 네트워크를 잘 아는 누군가가 생산 라인의 제어 명령을 변경한 것 같았다.

그날 저녁 집으로 돌아가는 길에(다행히 교통 신호 시스템에 더 이상 문제는 없었다) 저녁 뉴스에서는 오전에 있었던 교통 시스템 고장은 실제로 장난이었다는 보도가 나왔는데, 가담한 십대 중 한 명이 경찰에 전화로 자수해 밝혀졌다고 했다. 집에 도착했을 때 마리아는 그녀의 남편이 베이비 모니터를 상자에 넣고 있는 것을 발견했다. 그는 모니터의 보고되지 않은 백도어로 해킹되어 연결에 침입하는 방법이 인터넷에서 자유롭게 유포되고 있는 것을 알았다. 마리의 남편은 보다 안전한 다른 제품을 찾을 있을 수 있을 것으로 확신했지만 먼저 좀더 알아보기로 했다.

이러한 일이 실제로 일어날 수 있을까요? 아래의 내용에서 우리는 이 짧은 시나리오에서 일어난 모든 일들이 이미 어떻게 발생하게 되었는지 보게 될 것입니다. 또한 업계는 오늘날 검증된 방법을 사용하여 기술적으로 앞선 다른 시스템을 보호하면서 이러한 위험을 관리하고 최소화할 수 있는 능력을 갖추고 있다는 알게 될 것입니다.

이 백서에서는 기기와 시스템에 트러스트를 구축하는 데 사용할 수 있는 기법들을 살펴봅니다. 또한 기기(또는 사물), 정보를 저장하고 애플리케이션을 관리하는 서버, 그리고 시스템을 한데 묶는 네트워크를 포함하여 사물 인터넷의 물리적 인프라를 보호하기 위한 요구사항과 사용 가능한 기법들을 알아봅니다. 이렇게 구축된 안전한 물리적 인프라는 IoT에 의해 수집되고 사용되는 개인 정보와 데이터를 보호하는 정책을 성공적으로 구현하는 바탕이 됩니다.

* 가상의 인물

2. IoT의 혜택

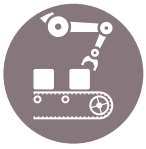
사물 인터넷이란 무엇일까요? 간단히 말하면 연결된 사물과 지능적인 서비스를 결합하는 것을 말하며, 자동차에서부터 의류, 공장의 기계에 이르기까지 모든 것이 네트워크에 연결됩니다. 연결되는 기기의 수는 다음 5년 간 매년 15-20%씩 증가해[1] 연간 매출이 수조 달러에 이르고 사물 인터넷이 침투하지 않은 시장은 찾기 어려울 것으로 예상됩니다.[2]

이러한 혜택들은 엄청나지만 위험한 측면을 동시에 갖고 있습니다. 공장, 가정, 교통 그리고 도시에서 대해 원격으로 이루어지는 지능적인 모니터링과 제어는 효율과 안전을 증대시킬 수 있습니다. 하지만 이와 같이 강력한 도구가 악의적인 집단에 의해 중요한 공공 인프라나 개인의 사적인 시스템을 파괴하는 데 악용됨으로써 위험하고 높은 비용이 초래되는 결과를 발생시킬 수 있습니다.

먼저 IoT의 혜택을 살펴보겠습니다. 지난 몇 년간 실제로 사물 인터넷을 구축한 결과 일상생활을 더 편리하고 안전하게 만들어주면서 상당한 절감과 함께 경제적 성과를 향상시키는 흥미진진한 기회를 목격하고 있습니다.

› 스마트 시티: 로스앤젤리스 시는 지자체의 가로등을 LED 램프로 교체하여 전기 요금을 연간 800만 달러 절감하고 있습니다(에너지 사용 60% 감소). 현재 네트워크 통제 센터에 연결된 무선 커넥티비티는 안전을 향상시키는 동적 시스템을 제공하면서 유지보수에 추가적인 절감을 가져다 줄 것으로 예상됩니다.[3,4]

› 스마트 빌딩: 뉴욕의 한 부동산 회사는 스마트 빌딩 기술을 도입해 단일 사무실 건물에서 약 100만 달러의 운영비를 절감하고 있습니다.[5] 이러한 절감은 빠르게 확대될 것입니다. 뉴욕 시는 도시의 75%에 달하는 에너지 관련 배출이 스마트 빌딩 기술을 이용해 보다 효과적으로 관리될 수 있을 것으로 보고 있습니다. 이 회사는 또한 자신들이 소유하는 더 작은 건물에도 이와 같은 절감을 실현하기 위해 기술 공급업체와 협력하고 있으며, 궁극적으로 주거용 주택에까지 이러한 기술을 적용하는 방법을 찾고 있다고 보도되었습니다.



› 스마트 공장: 한 인텔 칩 생산 공장에서 시행된 프로젝트는 단일 제품 라인 테스트 비용을 연간 300만 달러 줄였습니다. 이 파일럿 시스템은 기계, 센서 및 공장 직원으로부터 발생하는 정보를 분석해 제조 공정의 실시간 제어를 개선합니다. 공장에서 생산되는 모든 칩에 이를 적용할 경우 제조업체는 연간 3000만 달러를 절감할 수 있을 것으로 예측하고 있습니다. 유사한 IoT 및 빅데이터 분석 시스템을 다른 많은 복잡한 제조 공정에도 구현할 수 있습니다.[6]

› 스마트 홈: 오늘날 IoT 기기의 약 25%를 차지하는 스마트 홈 기기는 홈 자동화와 보안 애플리케이션이 성장을 주도하면서 매출이 2015년 610억 달러에서 2019년에는 4900억 달러로 증가할 것으로 전망됩니다. 아직 초기 단계에서 영향을 측정하기 어렵지만, 최근 보고서에 따르면 노년층과 장애를 가진 사람들에게 특별한 가치를 갖는 것으로 나타났습니다.[7]

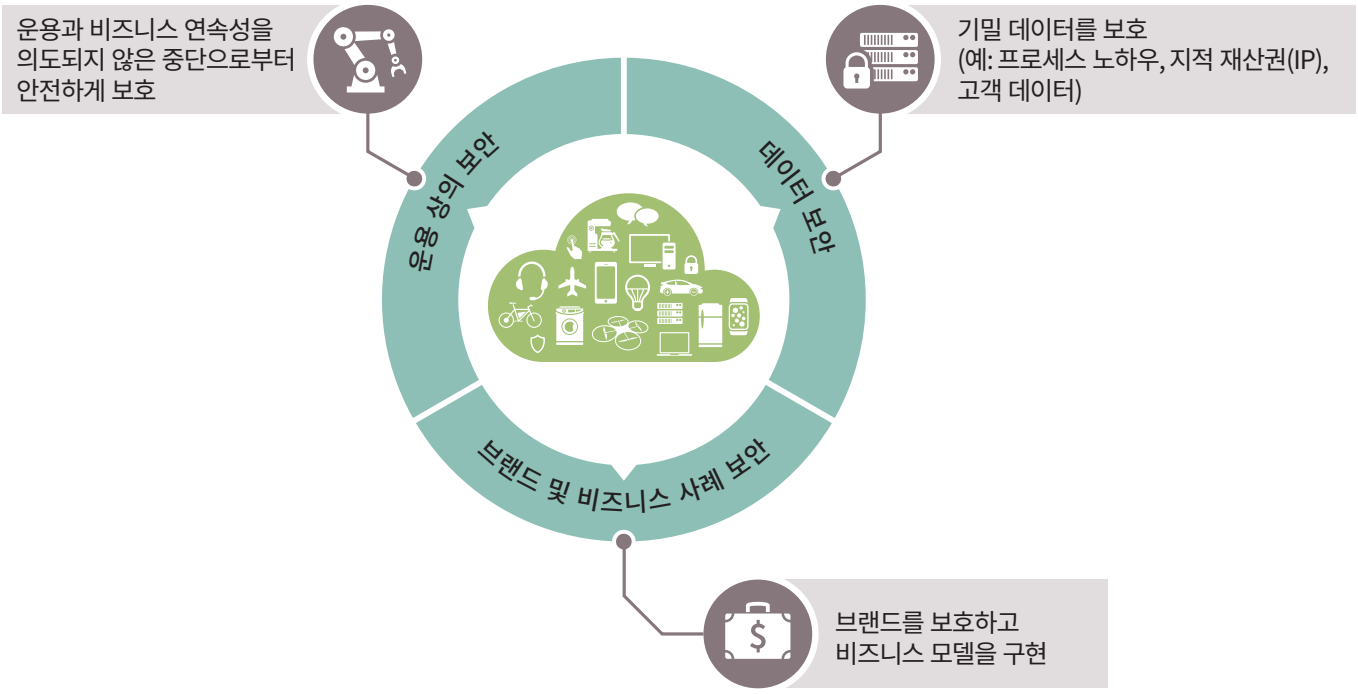
› 커넥티드 카: IoT가 개인의 안전에 어떠한 영향을 미치는지 가장 극적으로 보여주는 예가 커넥티드 카 기술 분야입니다. 한 보고서는 미국의 모든 차의 90%가 완전 자율(자율주행) 차량이 될 경우, 매년 420만 건에 달하는 사고를 피할 수 있게 되며, 이를 통해 21,700명의 생명을 구하고 4500억 달러의 관련 비용을 절약할 수 있을 것으로 추산했습니다.[8] 최근 보안 연구자들에 의해 커넥티드 카에 대한 공격이 성공할 수 있다는 것이 입증되고 있지만, 커넥티드 카의 향상된 안전과 개인의 생산성 증가, 그리고 자율주행 차량으로 전환함으로써 오는 스트레스의 감소는 이러한 위험을 증가한다고 간주됩니다.

인피니언은 사물 인터넷의 모든 경제 부문과 일상 생활의 모든 면에 걸쳐 이미 실현되었으며, 앞으로 실현될 혜택은 스마트한 상호 연결된 세계로의 전환을 불가피하게 만들 것이라는 데 동의합니다. 따라서 업계와 정책 결정자가 사물 인터넷의 보안 위험을 인식하고 이에 대처하는 것이 매우 중요합니다.

3. IoT의 위험

IoT의 위험은 모든 네트워크로 연결된 시스템의 위험을 그대로 반영합니다. 그러나 IoT는 매우 다양한 분야에 영향을 미칠 뿐 아니라 물리적 인프라와 서비스를 제어하는 역할을 하기 때문에 이러한 위험은 훨씬 광범위합니다.

IoT 기기나 시스템에 대한 공격이 성공할 경우 이러한 공격은 물리적 세계와 가상 세계에 모두 영향을 주므로 사용자, 기기 제조업체 및 서비스 제공업체에게 심각한 영향을 미칠 수 있습니다. 또한 개인 사용자 데이터뿐 아니라 노하우, 지적 재산권, 프로세스 인텔리전스와 같은 기밀 정보가 노출될 수 있습니다. 이 밖에도 운행 중단, 비즈니스 연속성의 훼손을 초래할 수 있으며 심지어 기업의 브랜드 이미지와 성공, 존속까지 위협할 수 있습니다.



보안이 필요한 이유

정책 결정자의 경우 IoT 위험 완화와 관련된 주요 관심은 공공의 안전과 개인 정보를 보호하는 데 있습니다. 따라서 산업 및 공공 인프라를 제어하는 네트워크 시스템을 우연적이고 악의적인 공격으로부터 보호하는 것이 매우 중요합니다. 일상 생활을 하면서 IoT 기기에 의해 모니터링되거나 사용자가 이러한 기기를 이용하여 자신의 재산을 모니터링하기도 하는 동안 개인에 대한 사적인 정보는 우연히 노출되지 않도록 보호되어야 하는 것은 물론 악용할 의도의 고의적인 도난으로부터 보호되어야 합니다.

교통 관리 시스템의 자동화는 교통 흐름을 향상시키고 이산화탄소 배출을 관리하면서 연료 비용을 절감할 수 있는 가능성으로 지방자치 단체에서 IoT 도입을 통해 공통적으로 초기에 추진됐던 프로젝트였습니다. 그러나 초기 구현에서는 시스템 보안의 기본 원리를 이행하지 못해 공격에 취약하다는 것이 드러났습니다. 2014년 미시건대 학생들로 구성된 화이트햇 팀이 실제 네트워크로 연결된 트래픽 신호를 통제해 교통 신호등(적녹황)의 상태를 원격으로 변경할 수 있다는 사실을 발견했습니다. 출고 당시의 기본 설정은 변경되지 않은 상태였고, 네트워크 명령은 암호화되지 않은 것으로 밝혀졌습니다.[9]

2014년 12월 독일 연방정보보안국에서 제철소에 발생한 사이버 공격을 보고했습니다. 확인되지 않은 공격자들은 공장 사무실의 컴퓨터 네트워크 침입을 시작으로 산업 제어 네트워크를 손상시키고 용광로를 제때에 끄지 못하게 함으로써 "막대한 피해"를 입혔습니다.[10] 이 공격 성공에 대한 자세한 내용은 알려지지 않았지만, 현재 유사한 자동화 시스템을 갖춘 회사들이 보안 지침과 실제적인 이행을 면밀히 검토하는 자극제가 되고 있습니다.

고객에 공급되는 전력을 중단시킨 공격은 이러한 종류로는 최초로 2015년 12월 말 우크라이나의 전력회사에 의해 보고되었습니다. 최소 한 곳의 우크라이나 전력공급회사의 8만 명이 넘는 고객이 몇 시간 동안 전력 공급을 받지 못했습니다. 정전의 원인이 아직 조사 중에 있지만, 전력회사 내부 시스템을 통제하기 위해 세 가지 다른 전략이 사용되었던 것으로 보아 치밀한 사전 계획이 있었던 것으로 추정됩니다.[11]

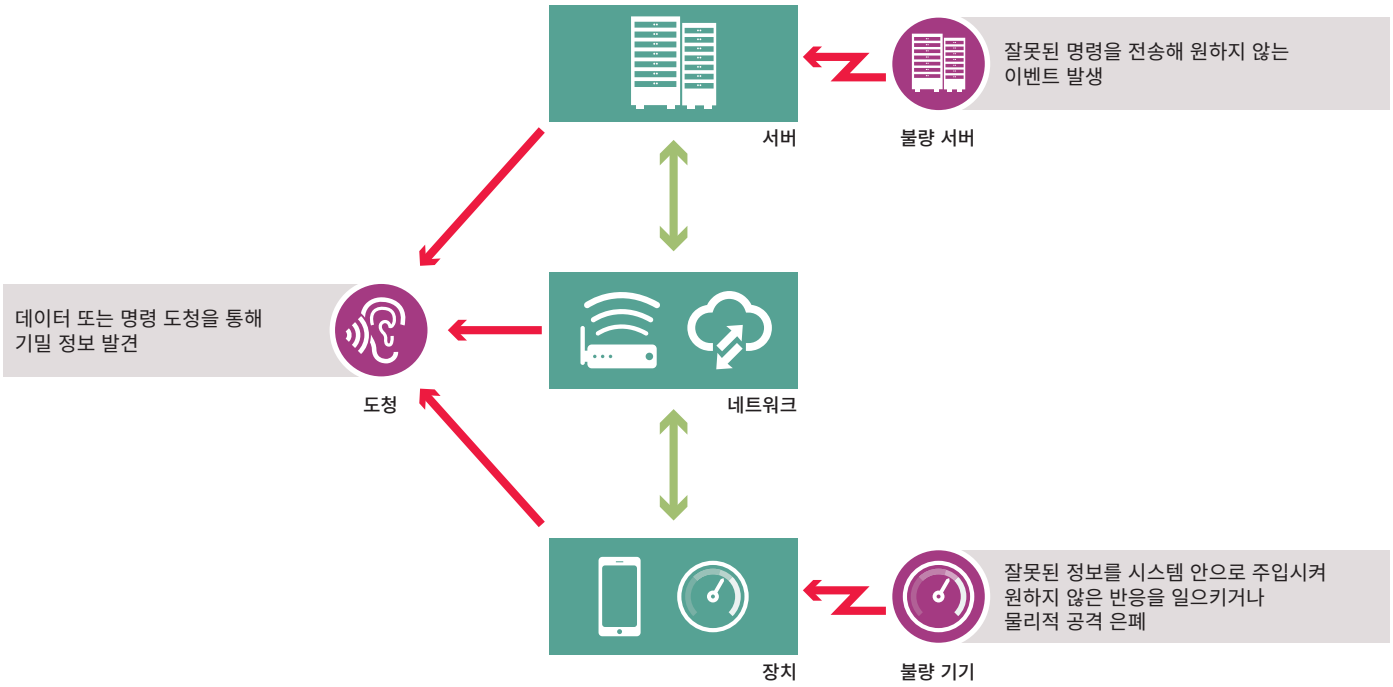
홈 모니터링 및 보안용 사물 인터넷이 급격히 확산되고 있지만, 보안을 위한 설계 원칙이 이를 따라가지 못하는 것으로 나타나고 있습니다. 2015년 여름 보안 연구자들이 취약성 조사를 실시했으며[12], 테스트한 인터넷 연결 베이비 모니터 제품들은 9개 중 1개는 보안에 심각한 결함이 발견되었습니다. 모든 카메라는 침입자가 접근할 수 있는 백도어를 가지고 있는 것으로 나타났습니다. 그 밖의 보안 결함으로 디폴트 비밀번호 사용, 쉽게 접근할 수 있는 인터넷 포털, 암호화 결여 등이 지적됐습니다. 해커들은 수 천 개의 발견된 안전하지 않은 웹캠을 알려주는 웹 사이트들을 누구나 볼 수 있게 만들어 놓고 있습니다.

매일 사용하는 기기를 인터넷에 연결할 때 발생할 수 있는 위험의 마지막 예는 2014년 초 실리콘밸리의 연구원들에 의해 보고되었습니다. 한 달 간의 스팸 메시지 조사에서 연구원들은 스팸 메일을 추적하여 해킹된 냉장고를 포함하여 스마트 가전 기기가 스펨 메일을 보내는 데 이용되고 있는 것을 알아냈습니다.[13] 하지만 소비자들이 인터넷에 연결된 가전 기기의 보안 상태를 알거나 유지하는 것은 가능하지도 기대할 수도 없으며, 사용자에게 이를 요구해서는 안 됩니다. 사물 인터넷의 가전 기기와 다른 기기들은 제품의 전체 수명 동안 지속되는 보안 조치를 갖춰 설계되어야 합니다.

4. 리스크 관리 및 감소

IoT와 관련된 위험의 유형은 애플리케이션(스마트폰, 인더스트리 4.0, 커넥티드 카, 정보통신 기술 등)에 따라 다양합니다. 하지만 공격 방법은 시스템의 범위에 걸쳐 공통됩니다. 도청 공격은 정보 발견을 목표로 하며, 발견된 정보는 이후의 공격에 사용될 수 있습니다. 다른 공격들은 서버를 파괴하거나 가장하여 잘못된 명령을 전송하고 원하지 않는 반응을 일으키거나 물리적 공격을 숨길 의도로 장치로부터 잘못된 정보를 주입하는 것을 포함합니다.

IoT에 대한 보안 위협



도청의 영향은 IoT 애플리케이션에 따라 달라집니다. 개인의 경우 개인 정보에 대한 침해는 개인적으로 치명적인 피해로 이어질 수 있습니다. 산업 스파이 성격의 공격이라면, 지적 재산권의 탈취 또는 공장이나 기타 운영에 대한 공격의 전초가 될 수 있습니다. 거짓 명령의 주입은 주택 거주자들에게 피해를 주고, 기업에게는 상업적 손실을 초래하고, 중요한 인프라에 심각한 손상을 입힐 수 있습니다. 반대로 장치에서 네트워크로 잘못된 정보를 주입하게 되면 쉽게 부정적인 영향을 미칠 수 있습니다.

IoT의 위험이 다른 네트워크 기술을 반영하듯이 디지털 시스템을 보호하기 위한 적절한 보안 대응이 입증되고 있으며 비교적

잘 이해되고 있습니다. 모든 IoT 보안에 적용 가능한 단일 솔루션은 없지만 다양한 많은 애플리케이션 시나리오에 걸친 접근 방법에서 공통적인 요소들이 있습니다. 모든 경우 보안의 목표는 디지털 정보의 인증되지 않은 읽기, 복사 및 분석을 방지하고, 보호되는 시스템의 직접적인 조작을 차단하는 데 있습니다. 이것은 소프트웨어 방식에서부터 견고한 하드웨어 기반 보안에 이르기까지 광범위한 기법을 통해 달성할 수 있습니다. 하드웨어 기반 보안은 특히 정교한 자원에 접근하는 악의적인 집단에 의한 고의적인 공격에도 견디도록 설계됩니다.

위험 평가

IoT 보안은 시스템 또는 시스템에 포함된 정보에 대한 전반적인 위험이 증가함에 따라 인가되는 보호 수준도 증가하는 위험 기반 방법을 사용하여 평가해야 합니다. 확장 가능한 보안 구현은 네트워크의 엣지에 더 단순하고 저렴한 장치를 분리시키고 중요 지점에 더 높은 수준의 보안을 구축하는 방식으로 각각의 장치를 보호하도록 설계할 수 있습니다.

위험 분석은 또한 전체 네트워크 시스템과 함께 이러한 시스템에 연결되거나 연결될 수 있는 많은 장치들에 대한 보안을 고려해야 합니다. 통신 네트워크에 장치를 연결하는 경우 모든 연결된 장치는 공격 표면이 될 수 있습니다. 심지어 무선 또는 유선 링크를 통해 제어되는 간단한 스마트 전구조차 IoT 시스템에 골칫거리가 되거나 보다 심각한 공격의 진입 지점이 될 수 있습니다. [14]

임베디드 시스템을 위한 보안 분야의 30여 년에 걸친 경험으로 인피니언과 고객사는 소프트웨어에만 의존하여 악의적인 공격으로부터 시스템을 보호하는 방법은 개별적인 장치뿐 아니라 보다 큰 네트워크 시스템을 위험에 빠뜨릴 수 있다는 것을 알고 있습니다. 하드웨어 보안은 IoT를 구성하는 많은 다양한 장치의 위험 수준에 적합한 중요 보호 계층을 제공합니다. 이러한 핵심적인 계층은 “루트 오브 트러스트(Root of Trust)”라는 개념을 중심으로 구성됩니다. 루트 오브 트러스트는 컴퓨터 칩에 상주하면서 메모리 및 처리 환경을 제공하는 보안 영역으로 시스템의 나머지 부분과 분리됩니다. 루트 오브 트러스트는 악의적인 공격으로부터 차폐되므로, 보호하는 컴퓨팅 시스템의 다른 운영 계층에 대한 보안을 제공합니다.

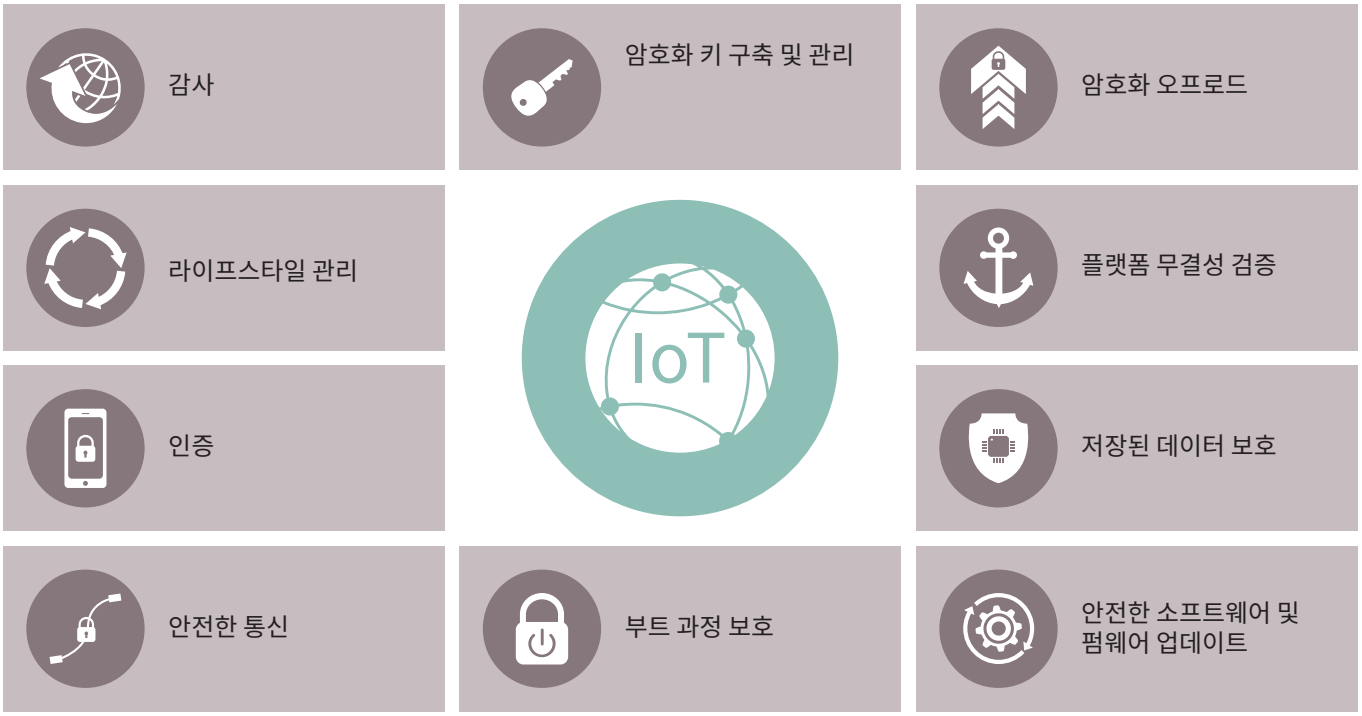
5. IoT 보안을 위한 최상의 방안

IoT를 위한 보안은 세 가지 주요 개념인 기밀성, 신분확인, 무결성을 중심으로 구성됩니다.
이들 개념은 다음과 같은 질문으로 나타낼 수 있습니다.

› 민감한 데이터의 전달과 저장이 보호되는가?
› IoT 시스템(디바이스, 서버 등)의 구성요소가 주장하는 그대로인가? 아니면 디지털로 위조된 것인가?
› 구성요소가 손상되거나 감염된 적이 있는가?

루트 오브 트러스트는 이러한 질문에 긍정적인 대답을 할 수 있는 최상의 방법입니다. 루트 오브 트러스트는 공격에 대비해 강화된 보안 칩이며, IoT 디바이스, 네트워크 또는 서버에 통합됩니다. 의도된 애플리케이션에 따라 사용되는 칩은 아래 그림에서 보이는 하드웨어 보안의 역할 중 일부 또는 전부를 이행하는 다양한 수준의 보호를 제공할 수 있습니다.

칩 기반 하드웨어 보안 역할



IoT 시스템에서 가장 낮은 수준의 위험은 소스를 검증하고 운영 데이터에 입력을 포함하는 일정한 종류의 게이트웨이나 로컬 서버에 센서 데이터를 단순히 중계하는 프로그래밍 불가능한 최종 노드가 될 수 있습니다. 이러한 수준에서도 사전 프로그래밍된 단일 ID를 갖는 저가 인증 칩은 장치의 전체 수명주기 동안 신분확인 방법을 제공합니다. 이러한 방법은 네트워크 엣지에서 복제된 장치의 확산을 방지하는 데 도움을 줍니다. 전송되는 데이터를 암호화해야 하거나 장치를 재판매 또는 재구성해야 하는 경우 추가적으로 키와 인증서에 대한 보호되는 저장을 고려해야 합니다.

장치와 서버 간에 흐르는 데이터와 명령은 도청과 잘못된 명령 주입 시도로부터 보호될 수 있도록 충분히 암호화되어야 합니다. 이를 위해서는 양쪽 끝에서 암호화 계산 기능이 필요하며, 이 기능은 위험 수준에 맞추어 조정할 수 있습니다.

가장 낮은 수준의 기능에서도 하드웨어 기반 보안은 암호화 메커니즘을 사용하여 비밀 데이터를 보호합니다. 암호화 알고리즘은 범용 MCU에서 실행하여 구현할 수 있지만, 장치 자체에 최소한 기본적인 탬퍼링 방지 기능과 암호화 기능을 갖추는 것이 바람직합니다. 이러한 보호는 일례로 신용 카드에 사용되는 칩에 이미 광범위하게 구현되어 있습니다. 이러한 칩은 스스로를 보호하고, 탬퍼링이 검출되면 메모리를 자동으로 삭제할 수도 있습니다.

IoT 보안은 시스템에 사용되는 모든 장치의 전체 수명주기 동안 보안을 제공하는 전체적 방법을 활용할 수 있습니다. 많은 수의 저가 장치를 사용하는 시스템에서 보안 하드웨어 공급망은 칩 제조업체로부터 어셈블리 지점까지 직접 칩 출하를 지원합니다. 사전 프로그래밍된 ID를 갖는 칩은 전원을 켜면 "무선으로" 자체 등록할 수 있습니다. 중앙 제어 지점에서 개별적인 장치에 보안 키를 탑재할 경우 침입과 파괴에 대해 더 쉽게 방어할 수 있습니다.

사용 가능한 IoT 보안 솔루션

이러한 모든 기법(탬퍼링 방지 회로, 인증, 암호화)은 이전에 다른 시스템에서도 사용되어 왔지만 IoT에는 아직 일상적으로 고려되고 있지 않습니다. 인피니언은 하드웨어 기반 보안이 더 나은 성능, 탬퍼링 방지를 포함한 향상된 보안, 보안 파티셔닝(운영 시스템과 애플리케이션 코드의 버그로부터 보호)와 같은 장점을 갖추고 있어 IoT에 적용하기에 매우 적합한 기술임을 확신합니다.

인피니언은 연결된 세계에 보안을 제공하는 선도업체로서 지난 25년 동안 전세계에 200억 개 이상의 보안 칩을 출하했습니다. IHS가 실시한 시장 조사에서 인피니언은 임베디드 보안 IC 분야에서 업계 1위를 차지했습니다.[15] 또한 인피니언은 다양한 시스템 요구사항을 만족하도록 다양한 제품군으로 구성된 광범위한 포트폴리오를 제공하고 있습니다.

임베디드 시스템을 위한 보안은 OPTIGA™ 제품군을 이용해 제공할 수 있습니다. 이들 제품군은 표준화된 풍부한 기능을 갖춘 솔루션인 OPTIGA™ TPM(Trusted Platform Module)과 턴키 또는 프로그래밍 가능한 솔루션을 제공하는 OPTIGA™ 트러스트 제품군으로 구성됩니다. 셀룰러 무선을 통한 안전한 M2M 통신을 위해 인피니언은 산업용 애플리케이션을 위한 SLM 76 및 SLM 97 SOLID FLASH™ 제품을, eCall(비상 전화) 서비스, 무선 소프트웨어 업데이트 및 C2C(Car-to-Car) 통신과 같은 자동차 애플리케이션을 위해 SLI 76 및 SLI 97을 제공합니다. 이들 보안 IC는 매우 견고하고, 넓은 온도 범위에서 동작하며, 산업용 및 자동차 표준을 만족합니다.

인피니언은 새롭게 떠오르는 스마트 웨어러블 기기 분야에 임베디드 보안 요소(eSE)와 부스트 NFC 보안 요소 IC를 제공합니다. 또한 인피니언의 엄선된 보안 IC는 안전한 온라인 인증을 위해 최신 FIDO 1.0 규격을 지원합니다.

임베디드 시스템을 위한 보안 솔루션
(OPTIGA™ TPM 및 OPTIGA™ 트러스트 제품군)

보안 컨트롤러
(산업용 SLM 76, SLM 97 SOLID FLASH™ 제품군 및
자동차용 SLI 76, SLI 97 SOLID FLASH™ 제품군)

임베디드 보안 요소, 부스트 NFC, FIDO, USB 토큰 및
RFID를 위한 혁신적 제품

보안 IC의 다양한 용도 및 인피니언의 제품 포트폴리오에 대한 보다 자세한 내용은 www.infineon.com/IoT-Security에서 확인하실 수 있습니다.

6. 참고문헌

[1] "The Internet of Things: Sizing up the opportunity," http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things_sizing_up_the_opportunity

[2] "Internet of Things By The Numbers: Market Estimates and Forecasts," http://www.forbes.com/sites/gilpress/2014/08/22/internet-of-things-by-the-numbers-market-estimates-and-forecasts/

[3] "Los Angeles to upgrade street lights with GPS," http://www.fiercewireless.com/tech/story/los-angeles-upgrade-street-lights-gps/2015-05-14

[4] "LA's Street Lights Can Now Be Wirelessly Controlled," http://gizmodo.com/las-street-lighting-will-be-controlled-by-a-wireless-ne-1696359821?utm_expid=66866090-62._DVNDEZYQh2S4K00ZSnKcw.0&utm_referrer=https%3A%2F%2Fwww.google.com%2F

[5] "New system lets buildings learn from energy use," http://www.capitalnewyork.com/article/city-hall/2014/12/8558111/new-system-lets-buildings-learn-energy-use

[6] "IoT and Big Data Analytics Pilot Bring Big Cost Savings to Intel Manufacturing," https://blogs.intel.com/iot/2014/09/28/iot-big-data-analytics-pilot-bring-big-cost-savings-intel-manufacturing/

[7] "IoT Innovations Offer Essential Benefits for People with Disabilities," http://www.aapd.com/resources/power-grid-blog/iot-innovations.html?referrer=https://www.google.com/

[8] "Driverless Cars: The Car Hack Security Challenge," http://destinhaus.com/driverless-cars-the-car-hack-security-challenge/

[9] Network World, August 20, 2014; http://www.networkworld.com/article/2466551/microsoft-subnet/hacking-traffic-lights-with-a-laptop-is-easy.html

[10] SecurityIntelligence.com; January 14, 2015; https://securityintelligence.com/german-steel-mill-meltdown-rising-stakes-in-the-internet-of-things/

[11] "Everything We Know About Ukraine's Power Plant Hack," Wired, January 20, 2016, http://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack /

[12] "Watch out, new parents – internet connected baby monitors are easy to hack,"http://fusion.net/story/192189/internet-connected-baby-monitors-trivial-to-hack/

[13] "What Do You Do If Your Refrigerator Begins Sending Malicious Emails?," http://www.npr.org/sections/alltechconsidered/2014/01/16/263111193/refrigerator-hacked-reveals-internet-of-things-security-gaps

[14] "Why Lightbulbs Will be Hacked," http://www.eetimes.com/author.asp?section_id=36&doc_id=1327843

[15] IHS TECHNOLOGY Insight Report
Embedded Digital Security Report – 2016
December 2015 ihs.com
Contacts
Sam Lucero, Sr. Principal Analyst
Sam.Lucero@ihs.com

Infineon Technologies AG

81726 Munich
Germany

www.infineon.com